

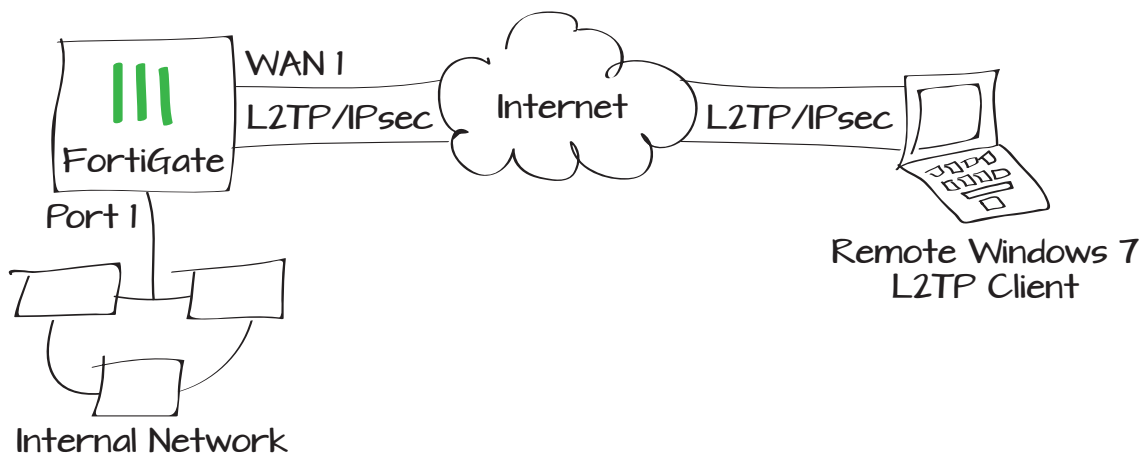
Configuring a FortiGate unit as an L2TP/IPsec server

The FortiGate implementation of L2TP enables a remote dialup client to establish an L2TP/IPsec tunnel with the FortiGate unit directly. Creating an L2TP/IPsec tunnel allows remote users to connect to a private computer network in order to securely access their resources. For the tunnel to work you must configure a remote client to connect using an L2TP/IPsec VPN connection. This recipe is designed to work with a remote Windows 7 L2TP client.



The FortiGate unit must be operating in NAT/Route mode and have a static public IP address.

1. Creating an L2TP user and user group
2. Enabling L2TP on the FortiGate
3. Configuring the L2TP/IPsec phases
4. Creating security policies for access to the internal network and the Internet
5. Configuring a remote Windows 7 L2TP client
6. Results



Creating an L2TP user and user group

Go to **User & Device > User > User Definition**.

Create a new L2TP user for each remote client.

Go to **User & Device > User > User Groups**.

Create a user group for L2TP users and add the users you created.

Enabling L2TP on the FortiGate

Enable L2TP on the FortiGate and assign an IP range for L2TP users.

Go to **System > Dashboard > Status > CLI Console** and enter the CLI commands shown here.

The **sip** indicates the starting IP in the IP range. The **eip** indicates the ending IP in the IP range.

User Name

☐ Disable

☒ Password

☐ Match user on LDAP server

☐ Match user on RADIUS server

☐ Match user on TACACS+ server

Name

Type ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest

Single Sign-On (RSSO)

Members

Remote authentication servers

Remote Server	Group Name
No matching entries found	

OK Cancel

```
config vpn L2TP
  set sip 192.168.10.1
  set eip 192.168.10.101
  set status enable
  set usrgrp L2TP_users
end
```

Configuring the L2TP/IPsec phases

On the FortiGate, go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1**. Set **IP Address** to the IP of the FortiGate, **Local Interface** to the Internet-facing interface, and enter a **Pre-shared Key**.

Enable all of the **DH Groups** and disable **Dead Peer Detection**.

When you are finished with Phase 1, select **Create Phase 2**. Name it appropriately and set it to use the new L2TP Phase 1.

Expand the **Advanced** options and specify a suitable **Keylife**. For example, **3600** seconds and **250000** KBytes.

Name

L2TP

Comments

Write a comment... 0/255

Remote Gateway

Dialup User

Local Interface

wan1

Mode

☐ Aggressive

☒ Main (ID protection)

Authentication Method

Preshared Key

Pre-shared Key

.....

Peer Options

☒ Accept any peer ID

☐ Accept this peer ID

☐ Accept peer ID in dialup group

Android_Users

P1 Proposal

1 - Encryption

3DES

Authentication

SHA1

2 - Encryption

AES128

Authentication

SHA1

DH Group

1 2 5 14

Keylife

28800 (120-172800 seconds)

Local ID

(optional)

XAUTH

☒ Disable

☐ Enable as Client

☐ Enable as Server

NAT Traversal

☒ Enable

Keepalive Frequency

10 (10-900 seconds)

Dead Peer Detection

☐ Enable

Name

L2TP_P2

Comments

Write a comment... 0/255

Phase 1

L2TP

Advanced...

P2 Proposal

1- Encryption

3DES

Authentication

SHA1

2- Encryption

AES128

Authentication

SHA1

☒ Enable replay detection

☐ Enable perfect forward secrecy (PFS).

DH Group

1 2 5 14

Keylife:

Both

3600 (Seconds)

250000 (KBytes)

380

The FortiGate Cookbook 5.0.7

Go to **System > Dashboard > Status > CLI Console**. In the **CLI Console** widget, edit the Phase 2 encapsulation mode using the CLI commands shown here.

Creating security policies for access to the internal network and the Internet

To ensure that policy-based IPsec VPN is enabled, go to **System > Config > Features**, turn on **Policy-based IPsec VPN**, and click **Apply**.

Go to **Policy > Policy > Policy**.

Create an **IPsec VPN** security policy to allow inbound and outbound traffic on wan1 by setting both the **Local Interface** and the **Outgoing VPN Interface** to **wan1**.

Set both the **Local Protected Subnet** and the **Remote Protected Subnet** to **all**.

Next to **VPN Tunnel**, select **L2TP** and **Allow traffic to be initiated from the remote site**.

```
config vpn ipsec phase2
    edit L2TP_P2
        set encapsulation transport-mode
    end
```



Policy Type	<input type="radio"/> Firewall <input checked="" type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> IPsec <input type="radio"/> SSL-VPN
Local Interface	wan1
Local Protected Subnet	all
Outgoing VPN Interface	wan1
Remote Protected Subnet	all
Schedule	always
Service	ALL
Logging Options	
<input type="radio"/> No Log	
<input type="radio"/> Log Security Events	
<input checked="" type="radio"/> Log all Sessions	
VPN Tunnel	
<input type="radio"/> Create New <input checked="" type="radio"/> Use Existing	
VPN Tunnel	L2TP
<input checked="" type="checkbox"/> Allow traffic to be initiated from the remote site	

Go to **Policy > Policy > Policy**.

Create a **Firewall** security policy allowing remote L2TP users access to the internal network.

Set the **Incoming Interface** to **wan1** and the **Outgoing Interface** to **internal**.

Set the **Source Address** to the L2TP tunnel range.

Go to **Policy > Policy > Policy**.

Create another **Firewall** security policy allowing **wan1** to **wan1** traffic so that clients connected with L2TP can access the Internet through the VPN.

Set the **Incoming Interface** to **wan1** and the **Outgoing Interface** to **wan1**.

Set the **Source Address** to the L2TP tunnel range.

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

wan1

Source Address

L2TP

Outgoing Interface

internal

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

wan1

Source Address

L2TP

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

Configuring a remote Windows 7 L2TP client

To connect to the FortiGate using L2TP, the remote client must be configured for L2TP/IPsec. The following configuration was tested on a PC running Windows 7.

On the Windows PC, create a new VPN connection.

Right-click on the new connection and select **Properties**, then modify the connection with the settings shown.

L2TP VPN Connection Properties

General

Options

Security

Networking

Sharing

Host name or IP address of destination (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):

172.20.120.81

First connect

Windows can first connect to a public network, such as the Internet, before trying to establish this virtual connection.

☐ Dial another connection first:

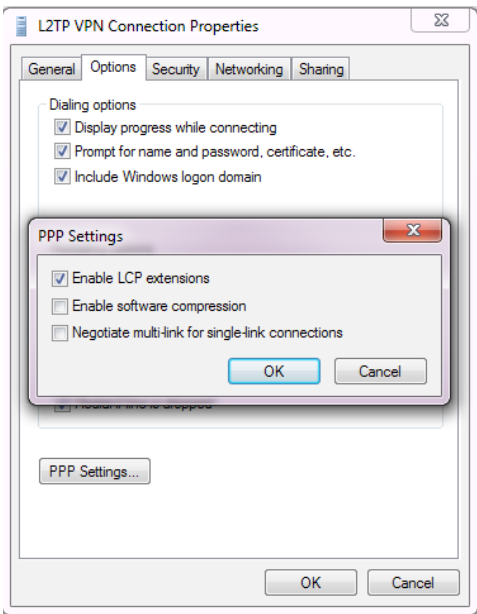
See our online [privacy statement](#) for data collection and use information.

OK

Cancel

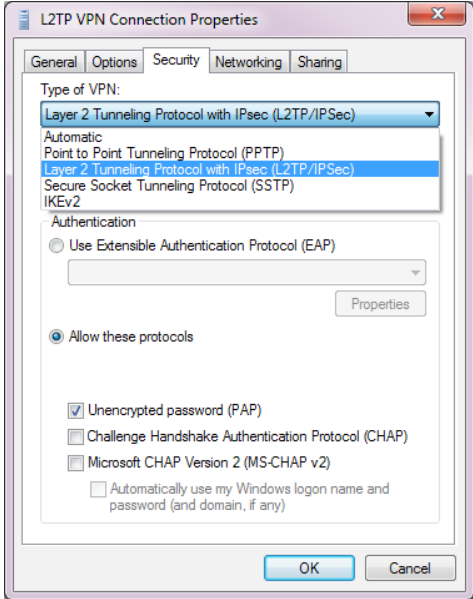
The **Host name** is the wan1 interface of the FortiGate unit that is acting as the L2TP/IPsec server.

Under the **Options** tab, enable **LCP extensions**.

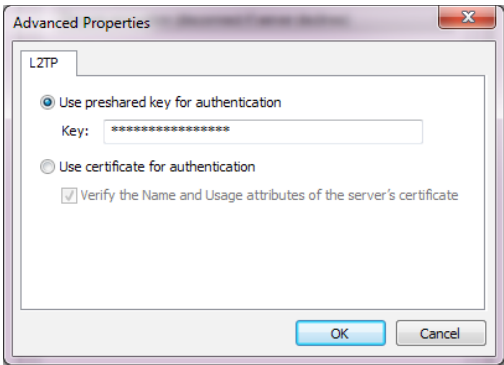


Under the **Security** tab, set the **Type of VPN** to **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)**.

Ensure that you allow only **Unencrypted password (PAP)** protocol. Disable other protocols.



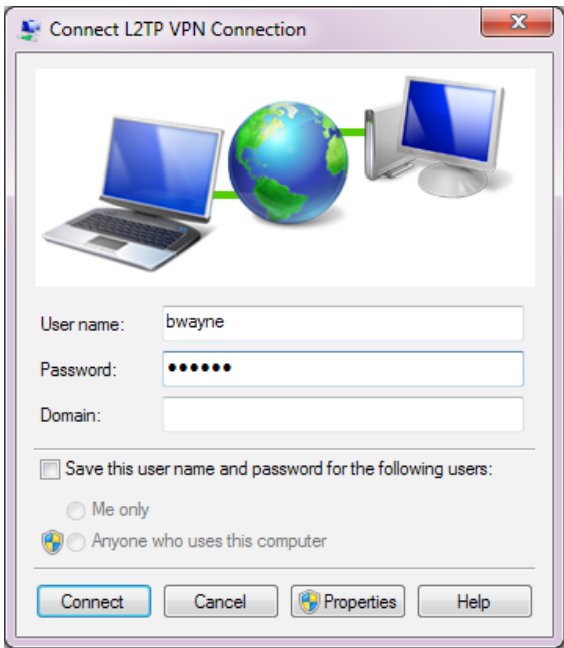
Click **Advanced Settings** and enter the pre-shared key you created in the Phase 1 configuration on the FortiGate.



Results

On the remote user's PC, connect to the Internet using the L2TP/IPsec connection you created.

Enter the L2TP user's credentials and click **Connect**.



Verify the connection in the GUI by navigating to **VPN > Monitor > IPsec Monitor**.

You can view more detailed information in the event log. Go to **Log & Report > Event Log > VPN**.

Select an entry to view the connection details, including **IPSec Local IP**, **IPSec Remote IP**, **VPN Tunnel** type, **User**, and more.

The **IPSec Remote IP** shown here should match the **Remote Gateway** shown under **VPN > Monitor > IPsec Monitor**.

Name	Type	Remote Gateway	Remote Port	Username	Timeout	Proxy ID Source
L2TP_0	Dialup	172.20.120.222	0		3584	172.20.120.81-172.20.120.81
Proxy ID Destination	Status	Incoming Data	Outgoing Data	Uptime		
172.20.120.222-172.20.120.222	Bring Down	552 B	0 B	3 seconds		

Level	Action	Status	
notice	negotiate	success	negotiate IPsec phase 2
notice	negotiate	success	progress IPsec phase 2
notice	tunnel-up		IPsec connection status change
notice	phase2-up		IPsec phase 2 status change
notice	install_sa		install IPsec SA
notice	negotiate	success	progress IPsec phase 2
notice	negotiate	success	progress IPsec phase 1
notice	negotiate	success	progress IPsec phase 1
notice	negotiate	success	progress IPsec phase 1
notice	negotiate	success	progress IPsec phase 1

Action	negotiate	Cookies	ba6132a63bde0998/b8f7fc6b07cdc7bb
Date/Time	13:13:15 (1380805995)	ESP Auth	HMAC_SHA1
ESP Transform	ESP_AES	Group	N/A
IPSec Local IP	172.20.120.81	IPSec Remote IP	172.20.120.222
Level	notice	Local Port	500
Log ID	37122	Message	negotiate IPsec phase 2
Outgoing Interface	wan1	Remote Port	500
Role	responder	Status	success
Sub Type	vpn	Timestamp	Thu Oct 3 13:13:15 2013
User	bwayne	VPN Tunnel	L2TP
Virtual Domain	root	XAUTH Group	N/A
XAUTH User	N/A		